PRIVACY AND ACCESS TO PUBLIC RECORDS IN THE INFORMATION AGE

By

Sol Bermann

Battelle Policy Day Working Paper 06 - 1

April 2006

FOSTERING *Thought* LEADERSHIP

Battelle

***The* Business *of* Innovation**

THE JOHN GLENN INSTITUTE

PUBLIC SERVICE & PUBLIC POLICY

PRIVACY AND ACCESS TO PUBLIC RECORDS IN THE INFORMATION AGE

By

Sol Bermann

Battelle Policy Day Working Paper 06 - 1

April 2006

Battelle Policy Day

February 7, 2006

A full-day conference, co-sponsored by Battelle Memorial Institute and the John Glenn Institute for Public Service and Public Policy, to examine the intersection of 21st century technology and personal privacy.

Abstract

Historically, public records, specifically court-related records, have had some measure of public accessibility. Similar to the right to an open court system, the notion of open records goes to the public's right to observe the goings-on of government which leads to government accountability.[2] At the Federal level, one guarantee of open records is embodied by the Freedom of Information Act.[3] At the state level, records are open or closed according to state law.[4] Online public record access brings a wealth of potential benefits ranging from greater government access and accountability to increased cost-savings and efficiencies. However, due to the presence of highly sensitive, personal data, an increase in public records access also brings potential dangers, including heightened risk of identity theft and frivolous snooping into the affairs of others. How can government embrace the opportunities provided by online public records, but also secure the privacy rights of its citizens?

There are four possible approaches to this public records policy dilemma:[5]

1. Provide the broadest access to public records by placing them on the Internet, unmodified from their current paper or electronic format. This maximizes access but minimizes privacy.

[1] The leading decision on a constitutional right of access is *Richmond Newspapers v. Virginia* 448 US 555 (1980) holding that the right of the public and press to attend criminal trials is guaranteed under the First and Fourteenth Amendments; and that absent an overriding interest articulated in findings, the trial of a criminal case must be open to the public. The reasoning behind this decision was based on the history of public trials, and how such openness promoted fairness (both real and perceived), and confidence and trust in the government as it exercised its duties.

In a recent case, the Supreme Court of New Hampshire reiterated this, stating that "[t]he public right of access to court proceedings and records predates the state and federal Constitutions and is firmly grounded in the common law." *The Associated Press et al. v. State of New Hampshire*, Supreme Court of New Hampshire, Dec. 30, 2005 (http://www.courts.state.nh.us/supreme/opinions/2005/assoc145.htm).

[2] In *United States Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749 (1989) the court described the public's right to access those government records that "she[d] light on the conduct of any Government agency or official," 489 *U.S.* at 773. In this case, the court weighed that interest against specific FOIA exemptions.

[3] The Freedom of Information Act, 5 U.S.C. § 552, As Amended By, Public Law No. 104-231, 110 Stat. 3048 (1996).

[4] For listings of relevant state law, visit: The Freedom of Information Center (http://foi.missouri.edu/citelist.html 1) and The National Freedom of Information Coalition's State and National Freedom of Information Resources (http://foi.missouri.edu/citelist.html).

[5] Three of these approaches are described in *Privacy and Access to Electronic Case Files in Federal Courts.* Office of Judges Programs of the Administrative Office of the United States Courts, Privacy and Access to Electronic Case Files in Federal Courts, December 15, 1999.

2. Review the data elements within the public record files and modify them to protect individual privacy interests (ex: redact social security numbers to help prevent identity theft). A middle ground approach.
3. Create a bifurcated records system that would limit online access to certain private or sensitive information, but leave the complete paper or electronic record available for public review at the record holder's office. Another middle ground approach.
4. Do not place any public records related to citizens online at all. This minimizes access, but maximizes privacy.

Expanding on lessons learned from the experiences of the Privacy and Public Access Sub-Committee of the Supreme Court of Ohio Advisory Committee on Technology and the Courts,[6] this paper will discuss how following approach #2, modifying public records laws and rules so that public record information is the same online and off-line, can increase governmental accessibility and accountability, create greater governmental efficiency, all the while retaining individual privacy.

I. Introduction

Electronic recordkeeping predates the Internet. For decades, public records were stored on mainframes, punch cards, and magnetic tape. The move to electronic records permitted easier and wider access to records that had always been available in paper format, in addition to allowing records to be compiled, copied and distributed in new ways. As technology evolved to desktops and software programs, public records did the same, albeit generally at a somewhat slower pace than the technological curve. While the speed of searching and the ability to download large datasets increased, citizens still needed to travel to the recordkeeping institution to gain access to the records themselves, a requirement that ensured practical obscurity[7] kept most sensitive, personal data private.

---

[6] The Supreme Court Advisory Committee on Technology and the Courts Privacy Subcommittee (http://www.sconet.state.oh.us/ACTC/subcommittees/privacy/).

[7] "Practical obscurity" is a concept describing the difference between the public records that might be through a search of courthouse files, county archives, or local police stations and a group of records, or summary there of, located in a single location (ex: the Internet). When all records were kept in paper form in disparate locations their contents were practically obscure. The term was first referred to in *United States Department of Justice* v. *Reporters Committee for Freedom of the Press*, 489 U.S. 749, 764 (1989).

The Internet changed this dynamic. Starting in the early 1990's, public records have been placed online.[8] The benefits of online public records are myriad. Online records: maximize accessibility; support the role of government; promote government accountability; and effectively use government resources and staff.

Most compelling is that online access grants all citizens 24 hour, seven day a week, 365 days per year access to public records. This heightened level of access serves to close digital divide and disability access issues. With computers in public locations, such as libraries,[10] becoming ubiquitous, and records available online all day, every day, citizens no longer have to take time off of work to go to a record holder office and make a request. For lower-income workers in hourly-wage jobs, this is particularly important. In addition, citizens with disabilities will no longer have to physically travel to the record holders to gain access to records.

Along with greater accessibility, online access also allows for greater searching and downloading capabilities. This leads to cost-savings, both real and in terms of time, for both the record holder and the citizen. When this cost savings is combined with the heightened accessibility, moving to an online public records system would seem to not only be a logical step, but one government and citizens should be actively working towards.

However, this sudden 24/7 access to public records often has been done with little to no modification of existing public records laws. This has led to privacy concerns ranging from citizen "snooping" into sensitive information (found in such records as divorce and custody

---

[8] Beth Givens, *Public Records on the Internet: The Privacy Dilemma,* April 19, 2002 (http://www.privacyrights.org/ar/onlinepubrecs.htm).

[9] Privacy and Public Access Subcommittee of the Supreme Court of Ohio, *Draft Policy for Public Access to Records Maintained by the Ohio Courts,* 15, Supreme Court of Ohio, June 8, 2005 (http://www.sconet.state.oh.us/ACTC/subcommittees/privacy/working_doc/DraftPrivacyPolicyNumbered_060805.pdf).

[10] In Ohio, free, public Internet access is provided by the Ohio Public Library Information Network (OPLIN), through Ohio's 251 independent local public libraries Reference Ohio libraries (http://www.oplin.org/main.php?Id=62&msg=).

[11] The types of records available from jurisdictions vary, but the information that may be available on a given individual (and a likely source of the information) can include:

- Name and address (land title)
- Home ownership and loan amount (land title)
- Size of home, price, physical description (land)
- Social Security Number (divorce decree)
- Political party registration and voting frequency (voter registration).

cases); to the safety of public officials, such as judges and police officers;[12] to identity theft.[1] This public outcry has, in turn, led to various government responses. These responses have ranged from the removal of online records;[14] to the creation of bifurcated systems of public records, where limited information is placed online;[15] to the "head-in-sand" option where the issue is ignored and record holders and managers opt not to place anything online for fear of a public backlash. All of these options force citizens to continue to travel to the record holder's offices to obtain the "real" public record. None of these responses serve the citizen in terms of efficiency or in shining a light on governmental operations.

Public records policy is at a crossroads where the law is unclear and policy is not evolving with technology.[16] In order to best serve citizen and government interests in access, accountability and privacy, public records law and policy must be modified so that same public records data held on paper or electronic format is also available via the Internet.

The remainder of this paper will more specifically address fundamental policy questions revolving around whether electronic records and their traditional paper counterparts be treated identically in terms of public access. And if so, what data currently freely available should be restricted? This will be followed by a brief overview of the practical considerations that an individual or committee should make when approaching these questions. Finally, conclusions and recommendations will be offered for how other entities may approach issues of electronic records, privacy, and public access.

---

[12] Merrill Douglas, *Privacy Concerns*, Government Technology, January 2, 2006 (http://www.govtech.net magazine/story.php?id=97730); Renee Gamela, *No exceptions for online records*, Utica Observer-Dispatch, January 6, 2006 (http://www.uticaod.com/apps/pbcs.dll/article?AID=/20060106/NEWS/601060314/1001/NEWS).

[13] Amy Benfer, *Http In Cincinnati*, Legal Affairs, March/April 2003 (http://www.legalaffairs.org/issues/March-April-2003/story_marapr03_benfer.msp).

[14] See: Jonathan Krim, *Public records present identity theft dilemma*, Washington Post, May 29, 2005 (http://www.post-gazette.com/pg/05149/511846.stm); *Should All Court Papers Go Online? The Debate Rages On*, Privacy Journal, December 2004 (http://www.findarticles.com/p/articles/mi_qa3872/is_200412/ai_n9473518); Kimberley Powell, *Identities for Sale: Governments Withdrawing Online Access to Public Records*, December 11, 2001 (http://genealogy.about.com/library/weekly/aa120601a.htm).

[15] This is being done in Virginia, Wisconsin, among other states. Privacy Journal, *Should all court papers go online? The debate rages on*, December 2004 (http://www.findarticles.com/p/articles/mi_qa3872/is_200412/ai_n9473518).

[16] Merrill Douglas, *Privacy Concerns*, Government Technology, January 2, 2006 (http://www.govtech.net/magazine/story.php?id=97730).

[17] This approach is being following in Arizona, Indiana, Maryland, and is the recommended approach for the state of Ohio. This is being done in Virginia, Wisconsin, among other states. Privacy Journal, *Should all court papers go online? The debate rages on*, December 2004 (http://www.findarticles.com/p/articles/mi_qa3872/is_200412/ai_n9473518).

I. Privacy and Access to Public Records: Practical and Policy Considerations

The dynamic of technology outstripping policy and the tension between the increased benefits from ease of access to public records via the Internet versus the threats to privacy occasioned by disclosure of intimate details sometimes contained in those records, boils down to two fundamental questions:

1. Should electronic records and their traditional paper counterparts be treated identically in terms of public access? And if so;
2. What public record information should be made private?

A. Electronic records accessed via the Internet should be the same as their traditional paper counterparts

There are myriad reasons for creating a policy where online records are the same as their paper counterparts. From a policy perspective, allowing Internet access to public records gives greater overall accessibility to the workings of government to *all* citizens, including lower-income citizens and citizens with disabilities, which bolsters government transparency by shining a brighter light on the workings of government. From a practical perspective, Internet-based electronic record systems represent greater efficiency and cost-savings, and when coupled with permission-based technology, they provide security and a high-level of functionality to all users.

1. Policy that Empowers Citizens and Government

Creating an environment that bolsters accessibility to public records for all citizens, especially options that bridge the digital divide and give greater access to the disabled and rural communities, should be considered a governmental imperative. More importantly, the enhanced accessibility offered by Internet-based electronic record systems leads to greater governmental transparency and accountability. Finally, creating such a system with policies and laws that value and protect the privacy of citizens and their personal data lends itself to greater citizen trust in government, which can, in turn, lead to yet more governmental transparency and accountability.

a. Accessibility

Making public records, with the same content as their office-based counterparts, available via the Internet will greatly increase public record accessibility. Citizens will no longer be forced to physically go to the proper government office during office hours, fill out forms, and wait as a government employee finds the proper record. This ease of accessibility serves *all* citizens, but greatly affects four specific communities.

- **Rural:** Placing public records on the Internet allows citizens to access records from home or other public computing centers. This is especially important for people living in rural areas where access to records would otherwise involve lengthy trips to government offices during business hours.
- **Lower-income:** Many people low-wage jobs cannot take time off work without losing pay. This can lead to unequal access to government services. Twenty-four hour online access to public records would alleviate this concern.
- **Disabled community:** The Americans with Disabilities Act (ADA) guarantees, among other things, equal opportunity for individuals with disabilities in public accommodations and state and local government services.[18] Access to public records is a government service.[19] Online public records mean that the disabled community will be able to access records from their home, thus mitigating the need to visit the record holder's office. This ease of access greatly contributes to fulfilling the guarantees of the ADA.
- **Attorneys/Pro Se:** Finally, having public court records available online will assist the legal system and the administration of justice. Attorneys that are solo practitioners or in small firms, and pro se defendants, will be able to more efficiently use their time by not having to make trips to the court for research.

---

[18] Americans with Disabilities Act of 1990, 104 STAT. 327, §§. 201-204 (1990); Americans With Disabilities Act Questions and Answers (http://www.usdoj.gov/crt/ada/qandaeng.htm).

[19] U.S. Department of Justice, Civil Rights Division, Coordination and Review Section, *Letter of Finding C030,* March 14, 1994 (http://www.usdoj.gov/crt/foia/lofindx.htm).

[20] Jim Cissel, former Hamilton Country, Ohio Clerk of Courts stated that "[i]f I take [the online records] away, it's kind of like taking the ramp away from the courthouse." Andrew Brandt, *Privacy Watch: Divorce and Other Court Records Broadcast by Browser,* PC World Magazine, April 2003 (http://www.pcworld.com/news/article/0,aid,109360,00.asp).

- Press/Media: For reasons similar to any of the preceding constituencies, the press is a zealous advocate for electronic access to public records. Searchable electronic access to the same information found in office-bound files also allows journalists to do their jobs better. Because of this, the Reporters Committee for Freedom of the Press supports a system that allows for both open access and privacy protection when needed.[21]

b. Transparency and Accountability

Simply put, increased accessibility to public records leads to greater government accountability. Online public records give more citizens a greater ability to observe the workings of government than traditional public record systems. More government transparency leads to increased government accountability. The more accountable a government is the more citizens will want to work with and trust in government. Ultimately, this should become a non-vicious circle where government becomes more efficient and accountable, which, in turn, creates a more responsive and empowered citizenry.

2. Practical Efficiencies & Cost Savings

Operationally, electronic records and the Internet are a case study in ease and efficiency. Government offices now have the ability to create, gather and disseminate records rapidly in one seamless system, often without even having to create a paper record.[22]

a. Creation

Electronic record systems allow for efficiency and cost-savings in a variety of ways. Data can be entered more quickly and accurately as the people most familiar with the data (be it government employees or citizens themselves) directly enter the data themselves. Additionally, electronic records systems mean that record systems and keepers are no longer wedded to static forms, as new forms, records and datasets can be created through data aggregation. Overall,

[21] The Reporters Committee for Freedom of the Press, *Electronic Access to Court Records: Ensuring Access in the Public Interest*, November 2002 (http://www.rcfp.org/courtaccess/index.html).
[22] Indeed, large amounts of records are now being created electronically and never exist in paper format. Benfer, *Http In Cincinnati.* For an example of such a system in operation, visit the Hamilton County, Ohio probate court web site (http://www.probatect.org/).

electronic record systems lead to increased efficiencies in the speed and accuracy with which data is entered, the time it takes to correct inaccurate data, and the time in which it takes for a records request to be fulfilled.

b. Distribution

Distribution and fulfillment of record requests are equally made more efficient and experience similar cost-savings. Software and middleware programs can categorize, catalog, and aggregate complex record sets that reside in a central data repository or across systems. The speed and efficiency of record request fulfillment using an electronic record system is increased when that system is linked to the Internet. Now citizens can make requests and receive records without having to interact with government staff, allowing these workers to be reallocated to increase efficiencies elsewhere.

c. Usage

Online electronic records give unprecedented flexibility in multi-level user access and usage. With access control systems,[23] sensitive data may be shown or suppressed depending on the level of permission given to the user. This makes it possible for a variety of users to have access to the same record but see it in permutations ranging from complete to very limited access.

For example, a judge would see the all data associated with a divorce record in order to make a judgment regarding custody or support; this would include psychological and medical tests, all financial data including bank account numbers and financial institutions, birthdates, social security numbers, etc. A Friend of the Court would see a more limited version of this record for purposes implementing child support policy. For example, medical and psychological testing or testimony may be redacted. Finally, the public at large would see "the public record," which would include whatever information the law allowed to be made public. This version of the record may suppress bank account numbers, social security numbers, and the birthdates of minors.

[23] Office of Information Security, Government of Hong Kong, *Information Security Glossary*, 2006 (http://www.infosec.gov.hk/english/general/glossary.htm#AccessControlSystem).

d. Storage & Maintenance

In addition to greater efficiencies inherent in creating, aggregating and distributing record, electronic data records are much cheaper to store and maintain. Now all data and records can be stored in electronic format on hard drives, CD-ROMs, or DVDs.[24] This means cost-savings in the size of the onsite physical plant needed to access public records, in addition to less personnel needed to maintain the records. As off-the-shelf software becomes less expensive and hardware and memory costs continue to plunge, all of these efficiencies will only continue to increase.

3. Dissenting Views

Not everyone is of the view that paper records should be the same as online public records. Critics point to two main reasons for keeping public records off of the Internet, either partially or in toto: identity theft and prying into the personal affairs of others.

Identity theft is a very well-documented problem that all states have now made a criminal offense.[27] Critics of online public records are rightfully concerned that sensitive data, including social security numbers and bank account information, will be placed online and made easily available for misuse. There is also concern that online public records will lead to virtual voyeurism as citizens snoop into the records of their neighbors and misuse this information.

Critics often point to practical obscurity as the solution, and offer two alternatives to making public records, with the same information as their paper counterparts, available via the Internet. The first is to not place any public records on the Internet. The second is to create a bifurcated record system where partial public records are placed online, while the "official"

---

[24] Many in the archival community support back-up microfilm copies for record preservation, especially as electronic storage media, hardware, and software change over time. Supporting this position is the transition in computing storage media, from punch cards to magnetic tape to portable media such as 8" inch disks to 5.25″ inch floppy disks, to 3.5″ inch floppy disks to CD-ROMs to DVDs. See Stewart Granger, *Emulation as a Digital Preservation Strategy*, D-Lib Magazine, Vol. 6, No. 10, October 2000 (http://www.dlib.org/dlib/october00/granger/10granger.html).

[25] The archival community would similarly support back-up microfilm copies for preservation purposes for similar reasons as above. That is, as software and hardware change there is a danger that media will not be reformatted or reformatted properly or will simply be incompatible with whatever the current trends are in hardware and software. With the acceptance of standard language mark-up languages, such as XML, this is rapidly becoming much less of a concern. See Granger, *Emulation as a Digital Preservation Strategy*.

[26] *Privacy Issue at Sealing of Court Records*, Science Daily, December 9, 2005 (http://www.sciencedaily.com/upi/?feed=TopNews&article=UPI-1-20051209-11063100-bc-us-openrecords.xml).

[27] National Conference of State Legislatures, *Identity Theft Statutes*, February 9, 2005 (http://www.ncsl.org/programs/lis/privacy/idt-statutes.htm).

record can only be accessed at the office of the record holder. Both "solutions" do a disservice to government efficiency and accountability.

As previously stated, online access to public records promotes efficiency and lack government accountability. Records are already being created and distributed in electronic format; the efficiencies and accessibility of the Internet are an extension of that. Additionally, sensitive personal data that does not directly serve the purpose of tracking the business of government may still be available, even if it may be more difficult to access. Staying bound to antiquated, traditional paper/office based-systems of recordkeeping out of fear is an ostrich-like exercise that does not serve the interests of government or citizens.

Others believe creating a bifurcated system of public records is the best solution.[29] Under this system, two records are created and available for distribution; the "official" public record is kept at the record holder's office and a "sanitized" online record is made via the Internet. This bifurcated system is poor solution for both practical and policy reasons.

Practically speaking, it is a burden on record holders to maintain two record sets of the same data. From a policy perspective, citizens are likely to find it confusing to have two different versions of the same record, an "official" public record kept at a government office, and an online version merely for information purposes. In addition, the sensitive, personal data is still available for misuse by those with the will to do so. Finally, all of the accessibility and accountability advantages gained by having one public records system are lost. Ultimately, a bifurcated records system does a disservice to both government and its citizens.

4. Conclusion

Holding back online public records is akin to trying to plug a dike that has long since broken. It is time to make decisions based on citizen need and government efficiency. The solution to privacy concerns surrounding the availability of public records on the Internet, such as identity theft, is simple. Create a single public record by redacting unnecessary, sensitive personal information from both office-bound (paper and electronic) and online public records.

---

[28] It should also be noted that people inclined to commit identity theft or snoop on their neighbors have the ability to do so, whether records are online or in an office, it is only the ease of access that is different.

[29] In 2001 in Florida, a committee of judges, lawyers, court officials and others recommended that the Florida Supreme Court impose a moratorium on public access to complete court documents via the Internet. Larry Keller, *Partial Ban Asked for Records on Net*, Daily Business Review, November 21, 2001 (http://www.law.com/jsp/statearchive.jsp?type=Article&oldid=ZZZI31JRBUC).

B. Determining what data in the public record should be made private

Each state has its own set of public records laws, so there is no single answer as to what information or data currently in the public record should be made private. There is, however, a simple balancing test that can be used in making such a policy determination (the process behind establishing a body to examine this question will be discussed in a brief case study in the next section).

The considerations in this balancing process are:

- Does the data in question shine a light on the workings of government?
    - o If the answer is yes, then one moves on to the next question.
- Is the data in question of a sensitive nature, such that disclosure of the data in question lead to potential individual harm?
    - o If the answer is "yes" to both questions, the next question is whether the privacy interest of the individual outweighs the public's need to know?

For example, social security numbers have become ubiquitous, unique individual identifiers. Social security numbers can provide data that distinguishes between *John Doe* the felon and *John Doe* the citizen with a clear record. As such, they could be considered data that is essential to shining a light on the workings of government, be it administering justice or any other number of tasks.

However, social security numbers also provide data that clearly can bring harm through their disclosure. Social security numbers are a prime target for people seeking to engage in identity theft.[30] On balance, when it comes to social security numbers, most indications are that the privacy interest of the individual outweighs the public's need to know and this is why federal and state legislation is banning their use as an identifier. [31]

As aforementioned, the answers to these questions and balancing test will vary state to state and even according to the branch of government that is the record holder. For example, the

---

[30] See: Identity Theft And Your Social Security Number, SSA Publication No. 05-10064, February 2004 (http://www.ssa.gov/pubs/10064.html); Hijacking your Social Security number, December 27, 2005 (http://www.bankrate.com/brm/news/pf/20051227al.asp); Jeff Romig, *More Privacy Protection,* South Bend Tribune, December 29, 2005 (http://www.southbendtribune.com/apps/pbcs.dll/article?AID=/20051229/News01/512290415/CAT=News01).

[31] See: *Summary of the HIPAA Privacy Rule,* Department of Health and Human Services, last revised may 2003 (http://www.hhs.gov/ocr/privacysummary.pdf); Sara Muri, *Drivers to get new ID numbers,* Daily Missourian, December 28, 2005 (http://columbiamissourian.com/news/story.php?ID=17662); Hillary Wundrow *New laws target identity theft,* Beloit Daily News, December 27, 2005 (http://www.beloitdailynews.com/articles/2005/12/27/news/122705news03.txt).

state Supreme Court of New Hampshire recently decided that the financial information people disclose in divorce cases is not entitled to wholesale privacy protection. The court stated that "a generalized concern for personal privacy is insufficient to meet the state's burden of demonstrating the existence of a sufficiently compelling era son to prevent public access."[32] What is important is that the protocols, decision-process and the actual decisions are clearly articulated and documented and that the subsequent access policies are clear, consistently applied, and not subject to interpretation by individuals. This is best guaranteed by bringing together a diverse group of people to engage in the decision-making process.

II. Case Study: Privacy and Public Access Sub-Committee of the Supreme Court of Ohio

The Privacy and Public Access Sub-Committee of the Supreme Court of Ohio was one of the first sub-committees formed by the Supreme Court of Ohio Advisory Committee on Technology and the Courts. Historically, in Ohio, most court records have been open[33] to anyone willing to come down to the courthouse and examine the files. The reason that court files are open is to allow the public to find out the status of parties to cases (for example, dissolution of marriage); to find out final judgments in cases; and to observe and monitor the workings of the judiciary.

As has been discussed, with the advent of the Internet, information in court records now can be available remotely, 24 hours a day, seven days a week. At the same time, not all of Ohio's courts have the same resources or the same level of technology, resulting in varying levels of access to records across courts in the same state. All of these circumstances require new access policies to address the concern that the proper balance is maintained between public access, personal privacy, and public safety, while maintaining the public's right to oversee the integrity of the judicial process.

In 2000, the Ohio Supreme Court appointed the Advisory Committee on Technology and the Courts. The Court charged it with recommending a strategy on how best to bring Ohio's courts into the digital age. In addition to dealing with such issues as hardware and software costs

---

[32] The Associated Press et al. v. State of New Hampshire. Supreme Court of New Hampshire (Dec. 30, 2005) http://www.courts.state.nh.us/supreme/opinions/2005/assoc145.htm; Beverly Wang, *Court: Divorce finances not subject to privacy law*, New Hampshire Union Leader, December 30, 2005 (http://www.theunionleader.com/article.aspx?headline=Court%3A+Divorce+finances+not+subject+to+privacy+law&articleId=105f93b6-c6fl-4b7d-8a75-249575967c09).

[33] Anderson's Ohio Online Docs, Availability of public records, § 149.43. (http://onlinedocs.andersonpublishing.com/oh/lpExt.dll?f=templates&fh=main-h.htm&cp=PORC).

and implementation, the Advisory Committee weighed problems and opportunities associated with a technological transformation of the court system. Chief among those issues was the tension between increased ease of access to court records via the Internet and threats to privacy occasioned by disclosure of intimate details sometimes contained in those records. Accordingly, in 2002, the Court formed a privacy and public access sub-committee to explore those conflicting values and to make recommendations on how to resolve them.[34]

The sub-committee worked under the following assumptions: l)cost and technology were not to be treated as barriers in making policy recommendation, 2)Ohio's "sunshine laws" give strong presumption that the documents in court files, unless sealed, are public records, 3)public access to case files promotes understanding of and confidence in the court systems, and 4)the judiciary has inherent authority to control the dissemination of case files, which may justify restrictions on access to electronic case files to protect privacy.

The sub-committee was made up of stake holders, including representatives from the, judiciary (both appellate and trial-level branches), clerks of courts, magistrates, the state attorney general, the state auditor, the press, academia, and advocacy groups. This diverse body guaranteed robust discussion, and rarely led to unanimity of opinion.[35]

The first decision the sub-committee made was that it was going to treat public records the same whether they were online or on paper. Ultimately, the sub-committee would be making recommendations that would affect state law and/or court rules of superintendence.

The next decision was to examine potentially sensitive data elements (ex: social security numbers, financial information, health information) and go through the balancing test as to whether it was information that should be kept in the public record. Despite the diversity of the members and the constituencies they represented, less than ten data elements were ultimately

---

[34] Privacy and Public Access Subcommittee of the Supreme Court of Ohio, Draft Policy for Public Access to Records, last updated June 21, 2005

(http://www.sconet.state.oh.us/ACTC/subcommittees/privacy/working_doc/DraftPrivacyPolicyNumbered_060805.pdf).

[35] One committee member had a standing objection to treating online and offline records the same. Others had more or less standing objections to any decision that removed any data from a public record.

recommended for removal from the public record. [36] At present, the subcommittee's draft policy is under review by the Chief Justice of the Supreme Court of Ohio.

III. Privacy and Access to Public Records Policy Recommendations

The creation of a single policy and framework pertaining to privacy and access to public records is crucial. The rise of the Internet offers the opportunity to reassess public records access and privacy from the ground-up and avoid patchwork or makeshift systems of recordkeeping by making online and offline records the same. Technology now allows for a seamless system, where online and offline records are identical, thus providing heightened public access, which leads to greater government efficiency and accountability; all while respecting individual privacy by limiting sensitive personal data.

There are practical steps to go through in the development of such a policy. First steps include, selection of a diverse committee from multiple stakeholders; identification of sensitive data elements that are in the public record; concurrent identification of the current body of local, state and federal law surrounding privacy and public access. Following identification of sensitive data elements and the relevant body of laws, the committee should examine which data elements, if any, should be removed from the public record and offer recommendations on which laws and rules should be modified. Finally, all recommendations should be made available for a public comment period before official action is taken.

To ensure that the policy is complied with and kept up to date, a variety of safeguards should be put in place. A standing committee should be appointed to regularly review the policy and make additional recommendations. A data commissioner should be appointed to assist government agency compliance and education. [37] Finally, a privacy ombudsman [38] should be

---

[36] Privacy and Public Access Subcommittee of the Supreme Court of Ohio, Draft Policy for Public Access to Records, last updated June 21, 2005 (http://www.sconet.state.oh.us/ACTC/subcommittees/privacy/working_doc/DraftPrivacyPolicyNumbered_060805.pdf). Note, even as the Subcommittee was working towards it draft policy, in September 2003 the Federal Judicial Conference amended its 2001 policy regarding criminal case files to allow remote public access to electronic files as long as specified personal identifiers were redacted. U.S. Courts, *Judiciary Privacy Policy Page*, August 2004 (http://www.privacy.uscourts.gov/default.htm).

[37] National data commissioners exist in all nations in the European Union, as well as Hong Kong, Argentina, Australia, Canada, among others.

[38] Some provinces in Canada have both a privacy commissioner and a privacy ombudsman. See: Manitoba Ombudsman's Office (http://ombudsman.mb.ca/access.htm).

appointed so that citizens have an independent body with which to address complaints and other grievances.

The growth of the information age should be a call to action or, at minimum, a wake-up call for government to bring policy in line with technological progress. The rise of electronic recordkeeping and the Internet can maximize government accessibility and efficiency, and secure the privacy of citizens. Public policy surrounding the right of citizens to demand openness and transparency from their government and the right to expect their private lives to remain private is not a zero-sum game where one side's gain is the other's loss. Redacting unnecessary, sensitive personal data from the public record and then mandating that public records at a government office are the same as the public records found online is the first step in the creation of a uniform public record policy that gives maximum public access while respecting individual privacy.

Appendix A: Questions Not Addressed:

What to redact from the public record?

As discussed in the body of the paper, the ultimate determination of what data to redact or exempt from the public record will be determined by a combination of state/local laws and rules, and hopefully by a body that examines the issue as described in the recommendations section. Aside from social security numbers and financial account numbers, other sensitive data elements that are often redacted are residential and family information of judges and police officers.[39]

Who controls public records?

It was the experience of the Privacy and Public Access Subcommittee that there were differing opinions about who controlled policy decisions regarding court records. The judiciary believed that, due to separation of powers, the judicial branch could decide make policy via rules of superintendence. Meanwhile, the legislature was drafting legislation that would affect all public records, including court records, which they generously put on hold pending the outcome of the subcommittee's recommendation. The subcommittee hopes to resolve this issue by having the court adopt rules of superintendence with supporting legislation that mirrors the court's rules.

Is it mandatory to post public records online?

At present, there is no Ohio law or rule that requires a court to maintain a web site. Therefore, it has been up to local court rules to post anything, public records included, online at all. Thus, a court may post everything, nothing, or somewhere in between to their web site. [40] One goal of the subcommittee was to create a standard public records access policy for all courts to follow. While the subcommittee could not require courts to post records online, the subcommittee did recommend that any public records posted online match those held at the court house.

---

[39] *State ex rel. Plain Dealer Publishing Co. v. Cleveland,* 106 Ohio St.3d 70, 2005-Ohio-3807. Holding that Police officer photographs are exempt from disclosure under the Public Records Act because they constitute "peace officer residential and familial information" which is exempted from the public record under R.C. 149.43(A)(l)(p) and (7)(b).

[40] For example, the Columbiana County Common Pleas and Municipal Court states that "[b]y local Court Rule, certain information does not display because of Federal Law and privacy concerns." (http://www.ccclerk.org/case_access.htm)

My personal point of view is that, for all of the reasons laid out in the body of this paper, courts should be required to maintain a web site and post all public records online. There are obvious cost and staffing consideration that go along with this, but costs of creating and maintaining a web site continue to plummet, and mandating that all courts be online within the next decade is a more than reasonable timeline.

Data brokers?

Data brokers[41] make bulk public records requests from local, state, and federal government agencies. They add information from commercial sources such as credit reports and consumer survey data, and then repackage them for sale to individuals and subscribers. While many data brokers claim they limit access to select professions such as law enforcement, media, debt collectors, employment background checkers, landlords, private investigators, and attorneys, the reality is that almost anyone can obtain access to these files. This has led to rising valid consumer worries regarding misuse and downstream abuse of data.

Until recently, data brokers believed that self-regulation was a more effective response to consumer concerns about data usage than legislation. However, after numerous data spills and data thefts (by everyone from data brokers to financial institutions to state and federal government),[42] leading information brokers are now in favor federal legislation that would preempt more stringent state laws.[43] This is a step forward and bodes well for data brokers, their clients, and, most of all consumers.

[41] Examples of information brokers include: LEXIS or Choicepoint.
[42] Tony Kontzer and Larry Greenemeier, *Sad State of Data Security*, Wall Street & Technology - InformationWeek (http://www.wstonline.com/showArticle.jhtml?articleID=175801687).
[43] Joseph Menn, *Data Brokers Press for U.S. Law*, L.A. Times, December 26, 2005 (http://www.latimes.com/business/la-fi-idlobby26dec26,0,6599609.story?coll=la-home-business). However, other news sources have differing opinions, see Larry Abramson, Despite Rash of Data Thefts, Laws Slow in Coming, NPR, December 27, 2005 (http://www.npr.org/templates/story/story.php?storyId=5071292).

Appendix B: Relevant Resources - Documents

Access and Aggregation: Public Records, Privacy, and the Constitution, Daniel J. Solove,86 Minnesota Law Review 6 (2002).

Developing CCJ/COSCA Guidelines for Public Access to Court Records: A National Project to Assist State Courts, National Center for State Courts and the Justice Management Institute, Martha Wade Steketee Alan Carlson, October 2003 (http://www.ncsconline.org/WC/Publications/Res_PriPub_GuidelinesPublicAccessPub.pdf)

Draft Policy for Public Access to Records Maintained by the Ohio Courts, Supreme Court of Ohio Privacy and Public Access Subcommittee, June 2005 (http://www.sconet.state.oh.us/ACTC/subcommittees/privacy/working_doc/DraftPrivacyPolicyNumbered_060805.pdf)

Financial Privacy in Bankruptcy: A Case Study on Privacy In Public and Judicial Records, Department of the Treasury, Office of Management and Budget, Department of Justice, January 2001 (http://www.treas.gov/press/releases/reports/bankrstudy.pdf)

Justice Information Justice Information Privacy Guideline: Developing, Drafting and Assessing Privacy Policy for Justice Information Systems, National Criminal Justice Association, September 2002 (http://www.ncja.org/pdf/privacyguideline.pdf)

Privacy and Access to Electronic Case Files in the Federal Courts, Office of Judges Programs of the Administrative Office of the United States Courts, United States Courts, 1999 (http://www.uscourts.gov/privacyn.htm).

Privacy and Public Registers', Roger Clarke, Address to the IIR Conference on Data Protection and Privacy, May 1997 (http://www.anu.edu.au/people/Roger.Clarke/DV/PublicRegisters.html).

Privacy Policy Development Guide, U.S. Department of Justice - Global Justice Information Sharing Initiative, January 2005 (http://it.ojp.gov/documents/Privacy_Guide_Final.pdf)

Public Access to Court Records: Implementing the CCJ/COSCA Guidelines Final Project Report, National Center for State Courts and the Justice Management Institute, Alan Carlson and Martha Wade Steketee, October 2005 (http://www.ncsconline.org/WC/Publications/Res_PriPub_PubAccCrtRcrds_FinalRpt.pdf)

Public Access to Electronic Case Files, Privacy Rights Clearinghouse and Electronic Frontier Foundation, January 2001 (http://www.privacyrights.org/ar/court2001.htm)

Public Records: Access, Privacy, and Public Policy, Robert Gellman, Center for Democracy and Technology, April 1995 (http://www.cdt.org/privacy/pubrecs/pubrec.html)

Public Records on the Internet: The Privacy Dilemma, Privacy Rights Clearinghouse, April 2002 (http://www.privacyrights.org/ar/onlinepubrecs.htm)

Appendix C: Relevant Resources - Web sites

4th Courtroom 21 Conference on Privacy and Public Access to Court Records, Courtroom 21, October 2005 - contains links to presentations on a variety of topics related to privacy and access issues, including presentations on a variety of state level initiatives from Florida, Minnesota, New Hampshire, Pennsylvania, and Texas, (http://www.courtroom21.net/privacy/reference.html)

EFF "Freedom of Information Act (FOIA) & Open Government" Archive, Electronic Frontier Foundation (http://www.eff.org/Activism/FOIA/)

Electronic access to court records: Ensuring Access in the Public Interest, Reporters Committee for Freedom of the Press (http://www.rcfp.org/courtaccess/intro.html)

Florida Public Records Guide, State of Florida (http://www.stateofflorida.com/Portal/DesktopDefault.aspx?tabid=13)

Freedom of Information Act, U.S. Department of Justice (http://www.usdoj.gov/04foia/index.html)

Judiciary Privacy Policy Page, U.S. Courts, updated August 2004 (http://www.privacy.uscourts.gov/)

Privacy and Public Access to Court Records: State Links, National Center for State Courts, last modified October 4, 2002 (http://www.ncsconline.org/WC/Publications/Tech_PriPubStatelinksPub.pdf)

Privacy and Public Records, Electronic Privacy Information Center (http://www.epic.org/privacy/publicrecords/)
Ohio Sunshine Laws, Office of the Ohio Attorney General - includes links to Ohio Sunshine Law updates and relevant news (http://www.ag.state.oh.us/site_map/sunshine_laws.htm)

Public and Government Records, Privacy Rights Clearinghouse (http://www.privacyrights.org/records.htm)

SearchSystems.net Public Records Directory - an example of a commercial public records aggregator and reseller web site (http://www.searchsystems.net/)

U.S. Department of Justice - Office of Justice Programs Information Technology Initiatives, U.S. Department of Justice (http://www.it.ojp.gov/index.jsp)